Remarks

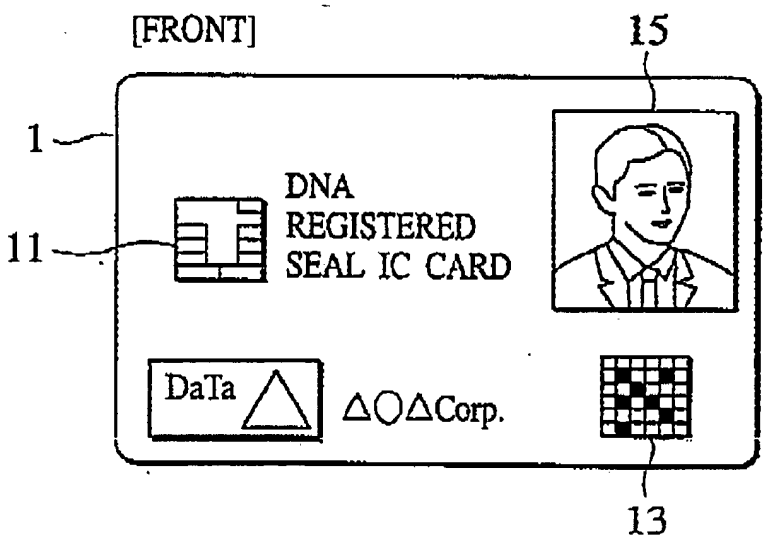
Claims 1-21 are pending and stand rejected. In view of the following remarks, the applicant respectfully requests that the rejection be withdrawn and the application be passed on to issuance.

Claim rejections – 35 USC §102

The Examiner rejected Claims 1-5 and 8-10 as being anticipated by US Pub. 2002/0129251 to Itakura.

Itakura discloses an identification card (1) that includes an integrated circuit (11) and a mark (13). Itakura, Fig. 1a, reproduced below, helps illustrate:

FIG.1A



The mark (13) is a two dimensional bar code printed with ink containing DNA from the owner of the card (1). Itakura, para [0034]. A DNA-ID code is generated from of the owner's DNA. Itakura, para [0084]. The two-dimensional bar code encodes the DNA-ID. Itakura, para [0053]. A secret key is generated by adding a random number to the DNA-ID. Itakura, para [0055]. A public key is

generated from the secret key. Itakura, para [0055]. The public key and the secret key are stored by the chip (11) on the identification card (1). Itakura, para [0055].

Claim 1 is directed to a method and recites the following acts:

1. encoding a public key in one or more ink strands;
2. embedding the one or more ink strands in a printing material; and
3. wherein the public key is uniquely associated with an electronic signature that is unique to a user.

In the previous response, the Applicant argued that Itakura does not teach "encoding a public key in one or more ink strands." In the current Office Action, the Examiner responds with the following:

> Itakura discloses a method of 15 authentication in which DNA-ID is placed on an authentication mark (13 of Fig 1A) as one or more ink strands. Within this DNA-ID, a public key is encoded. In an authentication process, the mark is read and the DNA-ID is decoded to reveal the public key. The examiner highlights the passage cited in the non-final action mailed 5/4/05:
>
> > "The DNA authentication mark 13 is read by the 2D bar scanner 33 using CCD 33a or the like, 20 **and the public key Y_A is obtained from the DNA authentication mark 13** at a public key analysis unit 51c of the client device 5. Then, the individual authentication is carried out at a matching unit 51a by matching the public key Y_A obtained from the DNA authentication mark 13 and the public key **YA** obtained from the CA and stored in a memory unit (DB) 51d" [0112].
>
> As explicitly disclosed in the passage, the public key is obtained from the DNA authentication mark. The DNA authentication mark is decoded at a public key analysis unit in order to reveal the public key.

It is true Itakura teaches that a public key is obtained from a DNA authentication mark (13). However, that public key is NOT encoded in the ink

used to form Itakura's authentication mark (13). That public key is stored by the chip (11) on the identification card (1). Itakura, para [0055]. Furthermore, the Applicant questions how Itakura's 2D bar scanner (33) could be used to reveal a public key encoded in an ink strand used to form authentication mark (13) on Itakura's identification card (1). A 2D bar scanner (33) is used to reveal data encoded in a 2D barcode and NOT data encoded in an ink strand of the ink used to form that bar code.

The Examiner's misunderstanding of Itakura is further illustrated by the following statement made in the present Office Action.

> The examiner also notes the contradiction in the applicant's argument. At the bottom of page 2, the applicant notes the following: "As discussed in Itakura, para [0112], the mark (13) can be later decoded using an optical scanner to reveal the DNA-ID and ultimately a public key associated with that DNA-ID". Here, the applicant states that the DNA can be decoded to reveal the public key. Yet, in the next paragraph the applicant concludes the exact opposite: "a public key is not encoded in that DNA".

The Applicant did NOT state that the DNA could be decoded. The Applicant stated that the mark (13) can be later decoded using an optical scanner to reveal the DNA-ID. The DNA-ID is digital information and is NOT encoded in ink strands of ink used to form authentication mark (13).

Itakura only discusses using ink that contains the DNA of a person to form an authentication mark (13) in the form of a 2D barcode. The pattern of that 2D barcode encodes the DNA-ID. The ink used to form the 2D bar code does NOT contain ink strands used to encode a public key. Consequently, Itakura does not teach encoding a public key in one or more ink strands and then embedding the one or more ink strands in a printing material.

For at least these reasons, Claim 1 is patentable over Itakura as are Claims 2-10 which depend from Claim 1.

Claim rejections – 35 USC §103

The Examiner rejected Claims 6 and 7 as being unpatentable over US Pub. 2002/0129251 to Itakura in view of USPN 6,312,911 issued to Bancroft. Claims 6 and 7 depend from claim 1 and include all the limitations of that base Claim. For at least the same reasons Claim 1 is patentable, so are Claims 6 and 7.

Claim rejections – 35 USC §103

The Examiner rejected Claims 11-14 as being unpatentable over USPN 6,397,194 issued to Houvener in view of US Pub. 2002/0129251 to Itakura in further view of USPN 6,312,911 issued to Bancroft.

Claim 11 is directed to one or more computer-readable media containing computer-executable instructions that, when executed on a computer, perform the following steps:

1. receiving an electronic document that has been converted from a paper document having a physical signature;
2. detecting one or more ink strands in ink used to create the physical signature, a public key being encoded in the one or more ink strands;
3. identifying the public key encoded in one or more of the one or more ink strands;
4. locating an electronic signature uniquely associated with the public key; and
5. attaching the electronic signature to the electronic document to create an electronically signed electronic document.

The Examiner contends that Bancroft and Itakura teach the second and third acts listed above. To the contrary, neither Bancroft nor Itakura teach or suggest detecting one or more ink strands in ink used to create the physical signature where a public key is encoded in the one or more ink strands. Those references also fail to teach or suggest identifying the public key encoded in one

or more of the one or more ink strands.

Bancroft discloses the use of DNA to encode messages and that such DNA could be incorporated into ink used to form a physical signature. That DNA could later obtained from physical signature and used for authentication purposes. *See, e.g.*, Bancroft, col. 10, lines 40-48. Bancroft does not teach or suggest encoding a public key in DNA which is then mixed with ink. Instead Bancroft merely teaches the use of DNA to encode messages.

As concluded above, Itakura merely teaches mixing a person's DNA into ink used to form a mark (13) on an identification card (1). A public key is not encoded in ink strands for that ink which is used to form the mark (13)

Furthermore, the Examiner mistakenly asserts that Houvener, col. 8, lines 1-8 teaches locating an electronic signature uniquely associated with the public key. That passage, reproduced below, mentions nothing of locating an electronic signature that is associated with a public key. It merely discusses digitally signing a record.

> In one preferred embodiment, the encryption processor 32 includes a digital signature processor 34 for attaching a digitally signed data element to each transaction data record before it is transmitted to the remote database site 20 over the communications link 12. In this manner, each transaction data record created by the transaction data processor 10 may be checked for origin and authenticity at the remote database site 20.

Houvener, col. 8, lines 1-8.

For at least these reasons, Claim 11 is patentable over the cited references as are Claims 12-16 which depend from Claim 11.

Claim rejections – 35 USC §103

The Examiner rejected Claims 15-21 as being unpatentable over USPN 6,397,194 issued to Houvener in view of US Pub. 2002/0129251 to Itakura in further view of USPN 6,312,911 issued to Bancroft and in further view of US Pub. 2002/0049614 to Rice.

Claims 15 and 16 depend from Claim 11 and include all the limitations of that base Claim. For at least the same reasons Claim 11 is patentable, so are Claims 15 and 16.

Claim 17 is directed to a method for converting a physical signature to an electronic signature and recites the following elements:

1. identifying a public key encoded in one or more ink strands contained in ink in which the physical signature was created;
2. locating the public key in an electronic signature database;
3. identifying an electronic signature in the electronic signature database that is uniquely associated with the public key; and
4. substituting the electronic signature in place of the physical signature.

Once again, the Examiner mistakenly contend that Itakura and Bancroft teach identifying a public key encoded in one or more ink strands contained in ink in which a physical signature was created. Bancroft discloses the use of DNA to encode messages and that such DNA could be incorporated into ink used to form a physical signature. That DNA could later obtained from physical signature and used for authentication purposes. *See, e.g.*, Bancroft, col. 10, lines 40-48. Bancroft does not teach or suggest encoding a public key in DNA which is then mixed with ink. Instead Bancroft merely teaches the use of DNA to encode messages. As concluded above, Itakura merely teaches mixing a person's DNA into ink used to form a mark (13) on an identification card (1). A public key is not encoded in ink strands for that ink which is used to form the mark (13)

For at least these reasons, Claim 17 is patentable over the cited references as are Claims 18-21 which depend from Claim 17.

Conclusion:

In view of the foregoing remarks, the Applicant respectfully submits that the pending claims are in condition for allowance. Consequently, early and favorable action allowing these claims and passing the application to issue is earnestly solicited. The foregoing is believed to be a complete response to the outstanding Office Action.

Respectfully submitted,
Travis J. Parry

By
Jack H. McKinney
Reg. No. 45,685

October 24, 2005